Ю. Баландін,
студент 5 курсу факультету
Комп'ютерних наук та інноваційних технологій,
Міжнародний гуманітарний університет;
керівник – канд. техн. наук, доц. В. В. Сергеєв

МОНІТОРИНГ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Реалізація загроз інформаційної безпеки (ІБ) може призвести до зупинення бізнес-процесів підприємства (закладу) внаслідок порушення цілісності та доступності інформації, появи фінансових втрат в результаті крадіжок конфіденційної інформації та втрати конкурентоспроможності на ринку товарів і послуг.

Тому проведення комплексного моніторингу інформаційної безпеки є нагальною потребою часу на кожному підприємстві або установі, особливо при наявності інформаційно-телекомунікаційних систем (ІТС), підключених до мережі Інтернет [1].

Як свідчить міжнародний досвід, організація та функціонування системи моніторингу можливе лише на підставі автоматизації усіх основних процесів виявлення інцидентів ІБ, проведення кореляційного аналізу значної кількості даних від різних підсистем (сканерів безпеки, між мережних екранів, маршрутизаторів, систем антивірусного захисту, систем виявлення вторгнень та ін.).

Можна викреслити наступні складові автоматизованої системи моніторингу ІБ:

- моніторинг працездатності апаратних засобів ІТС;
- моніторинг цілісності програмного забезпечення ІТС;
- моніторинг працездатності парольного захисту та захисту від несанкціонованого доступу в ІТС;
- моніторинг безпеки електронної пошти та ін.

Моніторинг працездатності апаратних засобів ІТС, наприклад, серверів, здійснюється у процесі їх адміністрування. Моніторинг цілісності програмного забезпечення (ПЗ) здійснюється при його завантаженні шляхом перевірки контрольних сум та цифрових підписів файлів та каталогів сертифікованих програмних засобів. Моніторинг працездатності парольного захисту та захисту від несанкціонованого доступу в ІТС передбачає періодичну перевірку паролів користувачів на кількість символів та виявлення слабких паролів за допомогою спеціалізованого ПЗ, фіксацію у системному журналі спроб невдалого входження користувачів в ІТС, виявлення роботи мережних сканерів, що спрямовані на дослідження та виявлення вражливостей ІТС та ін. Моніторинг безпеки електронної пошти полягає у перевірці вхідного повідомлення на наявність у ньому комп'ютерного вірусу. При виявленні наявності цього вірусу відправлення повідомлення повинно блокуватися. Також з метою блокування відправлення по пошті файлів що містять конфіденційну інформацію, необхідно передбачати заходи автоматичної перевірки змісту документа на наявність певних ключових слів, визначення адреси отримувача повідомлення, або перевірка його IP адреси.

Таким чином, моніторинг ІТС є складним та праце ємким процесом забезпечення інформаційної безпеки, який потребує певних фінансових витрат та залучення кваліфікованих фахівців [2; 3].

ЛІТЕРАТУРА

1. Лукацький О. В.. Системи виявлення атак / О. В. Лукацький // Банківські технології. – 1999. – № 2.
2. Гмурман А. І. Інформаційна безпека / А. І. Гмурман. – БІТ-М, 2004. – 387 с.
3. Устинов Г. М. Про проблему забезпечення інформаційної безпеки систем і мереж зв'язку / Г. М. Устинов // Метрологія та вимірювальна техніка в зв'язку. – 2000. – № 3.